韓國IT서비스學會誌
第12卷 第3號
2013年 9月, pp.151-164
http://dx.doi.org/10.9716/KITS.2013.12.3.151

정보사회에 있어서 '안전국가' 법규의 정립방향에 관한 소고

김 현 경*

A Study on the Direction of the Formulation of "Safe Country" Laws and Regulations due to the Development of Information Technology

Hyun-Kyung Kim*

■ Abstract ■

It is no doubt that information technology is the key factor of national safety. Information technology is positively useful for national security such as crime prevention and detection, criminal investigation, disaster management, and national defense. However, it might be a threat to the security as we saw in the examples such as '3.4 DDoS attacks' and 'Nong-hyup Computer Network Failure.' Although the effect that information technology makes upon the national security is immense, the current legal system does not reflect these changes well. National security should be kept during 'prevention-response-recovery' process regardless it is in the online on offline. In addition, public administration for national security should be based on laws. However, the current legal system is lack of legislative basis on cyber and physical disaster, and the laws on the response to disaster might cause confusing.

Therefore, this study examines the limitation of the current legal system on national security, and suggests directions for the development of the system based on the new establishment of the legal concept for 'national security'.

Keyword : Safe Country, Information Technology, Security in the Cyber Space, Legal system on National Security

논문투고일 : 2013년 07월 24일 논문수정완료일 : 2013년 09월 10일 논문게재확정일 : 2013년 09월 16일
* 한국정보화진흥원 책임연구원, 법학박사

1. 서 론

정보기술이 국가의 안전에 가장 중요한 영향을 미치는 핵심요인으로 작용하고 있다는 사실은 이제 별도의 논증이 필요 없는, 누구도 부인할 수 없는 사실이다. 정보기술은 범죄예방 및 탐지, 범죄수사, 재난 관리, 국방 등에 이용됨으로서 국가의 대내외적 안전에 긍정적으로 기능하기도 하지만 '3.4 DDoS공격', '농협 전산망 장애사건' 등의 예에서 알 수 있듯이 국민의 재산과 국가 안보를 위협하는 요인으로도 작용하게 된다. 이처럼 정보기술이 국가의 안전에 미치는 영향에도 불구하고 국가의 안전과 관련된 현행의 규범체계는 이러한 변화양상을 제대로 반영하지 못하고 있다. 국가의 안전은 온라인, 오프라인 구분 없이 '예방-대응-복구'가 끊김 없이 이루어져야 하며 국가 안전을 위한 공행정작용은 당연히 법규범에 근거하여 이루어지게 된다. 그러나 현행의 법규범은 사이버상의 재난과 물리적 재난을 연계하기 위한 입법적 근거가 미흡하며, 위기에 대한 대응법령체계 역시 혼란스럽다. 따라서 이하에서는 이러한 문제의식을 기반으로 국가의 안전에 대한 통일적·체계적 법규범 정립을 위한 시론적 연구로서 '안전국가'에 대한 새로운 법적 개념정립을 제안하고자 한다. 이를 바탕으로 '안전국가'에 부합하는 법규범 체계와 관련된 현행법의 한계와 개선방향에 대하여 고찰하고자 한다.

2. 정보기술의 발달과 안전국가

2.1 국가 안전 패러다임의 변화 : 사이버 위협

우리나라는 2010년 UN 전자정부 평가 세계 1위, 2011년 UN 공공행정상 세계 1위, ICT 기반 및 활용도 평가(일본 총무성) 1위 등 국가의 기반이 되는 많은 활동들을 정보기술에 의존하고 있다. 이러한 정보기술은 사이버 공간이라는 제 2의 공간을 생성시켰다. 사이버공간의 위협은 사이버 공간에 한정되지 않고 물리적 공간에도 직접적으로 영향을 끼친다는 점에서 그 파급효과는 핵전쟁에 버금갈 것이라는 우려도 나온다. 일례로 2007년 6월에 발생한 에스토니아와 러시아간의 사이버전에서는 에스토니아 수도 탈린에 있던 소련군 동상이 철거되자 대통령궁, 정부부처, 정당, 금융기관 등을 대상으로 대규모 사이버공격이 행해져 2개월간 행정업무가 마비되는 등 혼란이 야기되었다. 이후 나토는 에스토니아가 다시 사이버공격을 당하지 않게 하기 위하여 에스토니아에 유럽네트워크정보보안청(ENISA) 산하 사이버안전센터를 설립하였다. 에스토니아도 재발방지를 위하여 유럽 최초로 사이버 안보 전략을 수립하여 운영 중에 있다. 이후, 소련은 에스토니아에서 얻은 교훈을 토대로 그루지아와 사이버전을 수행하였다. '남 오세티아'를 둘러싼 영토분쟁으로 무력충돌이 확산된 그루지아 주요 정부 인터넷사이트가 러시아 비지니스 네트워크(RBN : Russian Business Network)로부터 수차례 무차별 DDoS 공격을 받아 초토화 되었다. 특히 중국은 사이버 공격이 고난도 해킹이 아니어도 근원지 추적이 불가능하고, 상대국의 네트워크 의존도가 높아 피해 확산이 용이하며, 국제법 미비로 국가 간 수사협조 및 사이버전(戰) 방어를 수행할 공조 체계가 어렵다는 것을 간파하여 물리적인 군사력과 함께 사이버 군사력을 확대해 나가고 있다[10].

한편 국가 기반시설을 연결하고 각 정보시스템에 영향을 주는 정보통신기반시설의 광범위한 침해사고는 국가 전반의 장애를 초래할 수 있다. 이러한 제어시스템을 포함한 정보통신시설의 사고는 석유, 환경, 원자력, 전력, 수자원 등 다양한 분야에서 발생하고 있으며, 인명을 포함하여 대규모의 피해를 야기한다[1]. 국내에서도 2009년에 발생한 청와대등 정부주요기관에 대한 7.7 DDos 공격을 비롯하여, 2011년의 3.4 디도스 공격, 4월12일의 농협전산망 마비사태 등 사이버 위험사태가 발생하여 사회적 혼란을 야기하였다.

경부고속도로가 1시간 사고로 막혀도 언론에서

더 이상 기사화하지 않게 일반화되어 있지만, 인터넷이 1시간동안 해킹으로 중단된다면 엄청난 사회적 이슈거리가 된다. 이제 강도에 의한 절취보다 인터넷 해킹을 통해 자신의 통장에서 돈이 인출되는 것에 더 불안해하는 시대에 살고 있다. 같은 위험에 노출되어 있음에도 불구하고 사이버 공간에서 사람들이 느끼는 감정은 더욱 민감할 수밖에 없다. 즉각적으로 인지될 수 없는 위험에 대한 불안감과 안전대책을 잘 모르기 때문에 어떻게 행동해야하는지 모르는 당황함이 야기될 수밖에 없기 때문이다.

한편 국가는 군대를 유지하고 경찰을 통해 치안을 확립하고 있다. 따라서 국민은 전쟁이나 재난 등 비상사태 발생 시 행동 요령에 의해 정해진 대피소로 이동하게 된다. 또한 적으로부터 공격을 받으면 적절한 대응을 통해 응징을 할 것으로 믿고 있다. 그러나 사이버공간은 매우 다른 양상을 보여준다. 우선 국가가 책임지고 해줄 수 있는 부분이 애매하다. 피해의 주체와 피해 받은 사람들이 명확히 구분되지 않는다. 또한 피해가 발생한 경우 피해 산정에도 어려움이 뒤따른다. 해커가 조직적일 수도 있고 개인적일 수도 있으며, 해커가 외국에 거주하는 경우 그를 검거하기 위한 국제적 공조도 쉽지 않다. 특히 해커는 지능적이므로 이러한 해커를 잡기 위한 사이버 수사관은 더욱 전문성을 가지고 있어야 한다. 해커가 죄의식을 갖지 않고 단순히 재미로 벌인 일인 경우 법적 처벌의 수위도 조정하기 어렵다[13]. 결국 기존 법률적 제도만으로 사이버공간의 규율기준을 마련하는 것이 불가능하다. 따라서 사이버 공간에 대한 규율은 국가의 안전을 위한 법률 체제에 있어서 중요한 변수이자 핵심요건이 된다.

2.2 국가안전에 있어서 정보기술의 순기능과 역기능

정보기술의 발달이 인간의 생활모습을 변화시키고 있다는 표현은 이제 더 이상 새로운 논증이 필요 없을 정도로 우리의 삶 속에서 그대로 드러나고 있다. 최근 정보기술이 인간의 삶에 가장 친숙하고도 큰 변화를 일으킨 것으로 판명되는 것이 스마트폰이다. 대부분 스마트폰으로 하루를 시작해 스마트폰으로 하루를 마감하는 생활이 일상이 되고 있으며, 친목관계, 음악・영화・게임 등 엔터테인먼트, 쇼핑, 독서, 길 찾기 등 모든 일상적인 활동에서 스마트폰은 마치 몸의 일부처럼 작동하고 있다. 이렇듯 정보기술의 개개인의 삶에 마치 대기처럼 자리 잡은 근저에는 인터넷 특히 모바일 인터넷의 보급이 중추신경처럼 작동하고 있기 때문이다. 정보기술은 더 이상 특정인, 특정 영역만의 사안이 아니며, 국민 개개인의 삶에 가장 중요한 기능을 함과 동시에 국가의 안전에 있어서 미치는 영향 또한 지대해 지고 있다[6].

우선 정보기술은 방범용 CCTV, 범죄자의 신상정보 DB를 통한 범인검거, RFID 센서를 통한 스쿨존 관리, 댐 등 사회기반시설의 실시간 관리 등을 가능하게 하는 등 범죄예방 및 탐지, 범죄수사, 재난 관리, 국방 등에 있어서 국가의 안전에 유용하게 활용되고 있다. 특히 태풍, 지진 등 재난 발생 시 모바일 및 소셜미디어를 활용한 비상통신, 경보 발송, 피해지 정보 및 피해자 정보 확인, 재난현장 대응 및 피해복구 지원 등 정보기술의 역할은 지대해 지고 있다. 동일본 대지진시 현장정보와 동영상, 사진 등의 제보와 상황중계, 구조요청, 복구지원, 실종자 찾기 등에 실시간 정보공유가 가능한 트위터가 유용하게 활용되었으며 급작스런 기상이변, 재해 등의 정보가 스마트폰을 통해 뉴스보다 빨리 전 세계에 전파되었다. 모든 기존 통신망이 불통되었을 때 트위터에 올라온 사진을 통해 아이티 지진의 참상이 최초로 공개되었으며, 우리나라의 경우에도 2010년 1월 서울지역 폭설 때 모바일 커뮤니티를 통해 폭설과 교통정보를 실시간으로 공유했던 사례가 있다. 이러한 맥락으로 정보기술은 국가의 안전에 큰 역할을 담당한다. 국방에 있어서도 정보기술은 미래 군의 모습을 변화시키는 가장 중요한 요인으로 인식되고 있으며

주요 국가들은 정보환경에 따른 군의 변화를 예측하고 이에 대비하기 위해 노력하고 있다. 그 결과 정보우위(Information Superiority)의 개념과 이를 추구하기 위한 네트워크 중심전(Network Centric Warfare)과 같은 새로운 군사작전의 개념이 등장하게 되었으며 현재까지 이러한 개념들을 보다 발전시키고 실질적인 소요로써 구체화하기 위해 지속적인 노력을 기울이고 있다. 국방에 있어서 정보기술의 적용은 시간과 장소에 구애받지 않고 원하는 정보를 작전수행인원에게 제공할 수 있는 환경을 구축한다. 고속 정보통신체계의 등장과 함께 C4I(Command and Control, Communication, Computer and Intelligence) 등 전장감시 및 통제체제가 획기적으로 강화될 것으로 전망된다. 실시간에 적군과 아군의 작전활동을 파악해 지휘 통제함으로써 광역화되고 분산된 군사력 전개 상황 하에서도 작전 템포가 획기적으로 빨라질 것으로 기대된다. 또한 제반 전투원과 무기체계 등의 전투요소를 통합적으로 운용할 수 있도록 응용체계를 개발하여 전력운용 효과를 극대화하고 이를 통해 정보우위를 달성하여 군사작전의 성공을 보장하고자 한다[23].

하지만 역기능도 존재한다. 2011년 9월 14일 오전 우리 영공을 지나가는 모든 민간항공기를 통제하는 항공교통센터(ATC) 비행자료 서버(주된 정보를 제공하거나 작업을 수행하는 컴퓨터 시스템)에 1시간 가까이 장애가 발생하면서 항공기 수십 대가 늦게 출발하는 사태가 벌어졌다. 또한 2012년 4월 28일부터 5월 13일까지 하루도 빠짐없이 북한이 수도권을 겨냥해 위성위치 확인 시스템(GPS) 교란 공격을 감행했으며, 이로 인해 대한민국의 항공기 676대, 선박 122척의 GPS가 불통돼 운항에 커다란 차질을 빚은 바 있다[9]. 이러한 까닭에 세계 각국은 자국의 생존과 이익을 위해 수많은 정보전을 치르고 있다. 과거 전쟁은 외부의 무력에 의해 정권이 전복되는 것이 대부분이었으나 최근 전쟁은 내부의 분열을 촉발시키고 심리적 공황사태를 만들어 사회적 혼란을 통해 정권이 붕괴되도록 만든다. 최근 리비아 사태가 가장 전형적인 방식이다. 2011년 1월 13일 벵가지에서 시작된, 카다피 리비아 국가수반 겸 국가평의회 의장의 퇴진을 요구하는 반정부 시위가 벌어졌다. 이 시위는 재스민 혁명과 이집트 혁명의 영향을 받아 그 규모가 확대되었고 결국 카다피 정권은 붕괴되었다. 지난 40여 년 간 철권 통지의 막을 내리게 한 결정적인 무기는 전투기, 미사일이 아닌 트위터·페이스북과 같은 소셜 네트워크를 통해 이루어진 정보 공유로 인한 시민 봉기였다. 결국 정보기술이 가장 큰 역할을 수행한 것이다. 카다피는 이러한 정보기술을 통한 정보 공유를 막고자 인터넷을 차단하였으나 정권을 지속적으로 유지하기에는 역부족이었다. 결국 정보기술을 어떻게 활용하느냐에 따라 무기가 될 수도 있고 좋은 문명의 이기로 만들어 갈 수도 있는 것이다.

이렇듯 정보기술은 국가의 안전에 가장 중요한 영향을 미치는 핵심요인으로 작용하고 있으며, 그 순기능을 살리면서 역기능을 억제, 예방할 수 있는 입법정책이 어느 때보다도 절실히 요구되는 시기라고 할 수 있다.

2.3 안전국가의 법적 개념 정립

'안전'의 사전(辭典)적 의미는 위험 원인이 없는 상태 또는 위험 원인이 있더라도 인간이 위해를 받는 일이 없도록 대책이 세워져 있고, 그런 사실이 확인된 상태를 뜻한다. 단지, 재해나 사고가 발생하지 않고 있는 상태를 안전이라고는 할 수 없으며, 잠재 위험의 예측을 기초로 한 대책이 수립되어 있어야만 안전이라고 할 수 있다. 그런 의미에서 안전이란 만들어지는 상태를 뜻한다[14]. 영어로는 safety 또는 security 등으로 표현할 수 있을 것이다. 그런데 상태적 개념으로서의 '안전'은 safety라고 표현하는 것이 적절하다. 이른바 safety는 안락 또는 평온한 상태나 환경을 의미하는 것으로 being well, peace, tranquility, ease, comfort, coziness 등의 복합적 의미를 내포하고 있다. 이에 반하여

security는 이러한 상태적 개념의 안전을 확보하기 위한 행동 등 동태적 개념이다. 따라서 security를 우리는 통상적으로 '보안'이라고 표현한다.

국가를 유지·존속시키기 위해서는 2가지 측면에서 국가의 공행정작용이 이루어져야 한다. 하나는 국민의 경제적 발전과 문화적 가치향상을 도모하는 것이고, 다른 하나는 국내의 치안을 유지하고 외적(外敵)으로부터 나라를 수호하는 일이다[8]. 후자를 헌법은 '질서유지'와 '국가안전보장'으로 각각 표현하고 있다. 국민의 기본권을 제한할 수 있는 근거로서 국가안전보장의 법적 의미에 대해서는 종래 질서유지의 개념에 포함되는 것으로 보았으나 1972년 헌법에서 처음으로 도입된 이래 통상 판례(헌법재판소, 1990. 4. 2. 89헌가113.; 헌법재판소 1992. 2. 25. 89헌가104.)와 학설은 "국가의 독립과 영토의 보전, 헌법과 법률 등 법규범의 효력유지, 헌법에 의하여 설치된 국가기관의 유지 등 국가의 안전을 확보하는 것과 동시에 사회영역도 포함하는 공동체의 안전을 확보하는 것"을 의미하는 것으로 새기고 있다[3]. 유신헌법에서 국가안전보장을 질서유지에서 분리하여 규정하였고 현행 헌법까지 그대로 계속되고 있다. 헌법재판소도 "국가의 존립·안전을 위태롭게 한다 함은 대한민국의 독립을 위협·침해하고 영토를 침략하며 헌법과 법률의 기능 및 헌법기관을 파괴·마비시키는 것으로 외형적인 적화공작 등을 일컫는다."라고 함으로써(헌법재판소 1992. 2. 25. 선고 89헌가113.) 이른바 국가안전보장은 외적 개념으로, 질서유지는 내부적 개념으로 이해하고 있다. 다시 말해서 대내적인 불안이나 위협에 대처하고 또는 이를 배제하기 위한 작용은 '질서유지'에 해당하고 대외적인 불안이나 위협에 대항하고 침략을 배제하기 위한 작용은 '국가안전보장'에 해당한다.

원래 국가의 존립·안전이란 영토의 불가침, 대내외적으로 헌법에 따라 행위 할 수 있는 능력, 주민의 생존근거를 포함하는 주민에 대한 안전의 보장을 의미하는 것이므로[32] '국가안전'은 국가의 대외적 불안이나 위협, 더 나아가서는 대외적 침략으로부터 국가의 안전을 보장하기 위한 것은 물론이고 국내적 불안이나 국내질서의 파괴, 또는 천재지변으로부터 사회의 안전을 보장하기 위한 것도 포섭하는 개념이다. 그러나 앞에서 살펴본 것처럼 우리헌법이 국가안전보장과 질서유지를 나누어서 규정하고 있고 헌법재판소 역시 국가안전은 외적 위협으로부터 국가를 보호하는 것으로 판시하고 있는 까닭에 '국가안전'이 그 본래의 뜻과는 달리 매우 좁은 의미로 이해되고 있다. 따라서 '국가안전' 또는 '국가안보'는 '외적 침략이나 위협으로부터 국가를 보호하는 것'으로 정의하는 것이 불가피하다. 물론 상태적 측면을 강조한다면 '국가안전'으로 반면에 동태적 측면에 초점을 둔다면 '국가안보'라고 표현할 수 있을 것이다.

결국 '국가의 안전'과 '안전한 국가'는 동일 개념으로서 다만 동태적 측면과 상태적 측면 중 어디에 중점을 두느냐의 차이밖에 없는 것으로 이해하는 것이 타당함에도 불구하고 현행 헌법과 관행화된 인식 등으로 인하여 새로운 용어의 정의가 불가피하다. 다시 말해서 '국가안전'은 외적 위협이나 침략으로부터 국가의 안전을 지키는 것으로 통용되고 있는 현실을 인정하고, 이러한 외적 안전은 물론이고 국민생활기반시설을 보호하고 천재지변 등의 재해를 예방·극복하는 등의 내부적 안전까지도 모두 포함하여 국민들이 안락·평온한 상태에서 헌법상 기본권을 향유할 수 있도록 하는 국가 공행정작용을 포괄할 수 있는 새로운 개념의 형성이 필요하다. 이러한 개념을 이른바 "안전국가"로 정의하고자 한다.

사실 앞서 언급하였듯이 사이버공간이 등장하면서 외부적 위협과 내부적 안전을 명확히 구분하기도 어렵다. 예컨대 내부의 폭력적 시위나 폭동이 외부적 세력에 의해 조정되는 것이라면 이를 외부적 위협으로 보아야 하는지 아니면 내부적 위험으로 보아야 하는지 불분명하다. 하지만 오프라인에서 발생하는 공격·위협이나 위험유발은 공격자 또는 위험유발자에 따라 외부적 침략인지 아니면 내부적 질서교란인지를 구분하려고 한다면 못할 바

도 아니다. 그러나 정보기술의 발달에 따라 사이버 공간에서는 내부·외부에 대한 물리적 경계는 더욱 희박하다. 국민생활기반시설이 컴퓨터에 의해서 제어되고 있는 상태에서 외부적 세력에 의한 해킹 등으로 이러한 기반시설이 파괴된다면 이는 '질서유지' 차원이 아니라 '국가안전보장'의 측면에서 접근해야할 것이다[9]. 그러나 실제에 있어서는 이러한 사이버공격이 내부적 소행인지 외부적 공격인지를 쉽게 찾아내기 어려울 뿐만 아니라, 사이버공격의 특성상 공격 이후에 공격자를 찾아 대응하는 것은 그 의미가 거의 없으므로 사전예방이 그 무엇보다 중요하다. 공격자를 미리 인지하고 외부적 공격과 내부적 위험에 각각 따로 대응한다는 것은 거의 불가능한 일이다. 사이버침해에 대해서는 헌법상 규정된 국가안전보장과 질서유지를 구분하여 국가 공행정작용을 발동하는 것이 사실상 어렵다는 것이다. 따라서 이러한 문제들을 모두 포섭할 수 있는 새로운 개념의 정립이 필요한 것이며, 새로운 개념을 '안전국가'로 정의하는 것은 매우 의미 있는 일이라고 생각된다. 즉 안전국가를 '모든 국민들이 안락·평온한 상태에서 헌법상 기본권을 향유할 수 있도록 하는 것'으로 정의한다면, '안전국가'는 국가의 존립과 국민들의 행복추구를 실현하기 위한 가장 중요한 기반적 국가정책이라 할 수 있다. 그 어떤 국가정책보다 후순위에 둘 수 없는 선택이 아닌 필수적 국가과제인 것이다.

3. '안전국가' 규범의 현황과 한계

3.1 안전국가 관련 법령현황

'안전국가'를 앞서 언급한 바와 같이 '외부적 안전과 내부적 안전을 포함하여 모든 국민들이 안락·평온한 상태에서 헌법상 기본권을 향유할 수 있도록 하는 것'으로 정의한다면, 안전국가 관련 법령은 그 범위가 매우 포괄적이며 기준에 따라 여러 가지로 분류될 수 있다. 물리적 안전과 사이버상의 안전 관련 법률로 구분할 경우 물리적 안전과 관련하여서는 「재난 및 안전관리 기본법」 등과 같은 기본법, 「시설물의 안전관리에 관한 특별법」 등과 같은 재난예방관계법, 「응급의료에 관한 법률」 등과 같은 재해응급대책관계법, 「재해구호법」 등과 같은 재해복구에 관한 법, 「소방공무원법」 등과 같은 조직관계법 등으로 분류할 수 있으며, 풍수해, 화재, 시설물 붕괴, 교통안전, 산업재해, 전염병 등과 같은 기타 사회적 재난 등과 같이 재난의 유형에 따라 법령을 분류할 수도 있다. 사이버안전과 관련한 법령의 현황은 「국가사이버 안전 관리규정」, 「전자정부법」, 「정보통신기반보호법」, 「개인정보보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」 등이 있다.

한편 조직법적 측면과 작용법적 측면에서 분류해 볼 경우 조직법의 대표적 법령은 단연코 「정부조직법」이다. 정부조직법에 의할 경우 안전국가의 기능은 국가안전보장에 관련되는 정보·보안 및 범죄수사에 관한 사무를 관장하는 국가정보원과 안전 및 재난에 관한 정책의 수립·총괄·조정, 비상대비·민방위 제도를 총괄하는 주체로서 안전행정부에 각각 분장되어 있다. 방송통신위원회는 「정부조직법」상 근거가 아닌 「방송통신위원회의 설치 및 운영에 관한 법률」 제11조 제1항 제2호에 따라 개인정보보호에 관한 사항을 관장하고 있다. 그밖에 「전자정부법」, 「정보통신망이용촉진 및 정보보호 등에 관한 법률」, 「국가사이버안전관리규정」에 근거하여 국가정보원, 안전행정부, 방송통신위원회가 각각 안전국가와 관련된 조직적 기능을 분담하고 있다. 그밖에, 사이버 테러에 대비한 조직으로는 경찰청의 사이버테러 대응센터(NETAN), 대검찰청의 첨단범죄수사과, 국가정보원과 국방부의 사이버사령부(「국방정보본부령」 제4조 제2항 제3호 : 사이버 군사작전의계획, 시행, 부대훈련 및 연구개발에 관한 사항을 관장하기 위한 사이버사령부) 등과 민간기관의 해킹 사고에 대비하기 위한 조직으로 방송통신위원회와 한국인터넷진흥원의 인터넷 침해사고대응반이 설치, 운영되고 있다[23]. 작

용법적 측면에서 볼 경우 안전행정부 소관의 「재난 및 안전관리 기본법」, 「전자정부법」, 「개인정보보호법」, 국토교통부 소관의 「시설물의 안전관리에 관한 특별법」, 소방방재청 소관의 「재해복구법」, 미래창조과학부 소관의 「정보통신기반보호법」, 방송통신위원회 소관의 「정보통신망이용촉진 및 정보보호등에 관한 법률」 등이 있다.

그밖에 국가기밀, 개인정보 보호, 전자서명·인증, 정보시스템 보호, 침해행위 처벌 등 안전국가와 관련된 영역별로 분류해 보면 법제현황은 다음과 같다. 국가기밀관련 법령으로는 「국가정보원법」, 「국가보안법」, 「보안업무규정」, 「군사기밀보호법」, 「국가정보화기본법」, 「전자거래기본법」, 「군형법」 등이 있고, 중요정보의 국외유출방지에 관한 법령으로는 「산업기술의 유출방지 및 보호에 관한 법률」, 「기술의 이전 및 사업화 촉진에 관한 법률」, 「민·군겸용기술사업 촉진법」, 「부정경쟁방지 및 영업비밀보호에 관한 법률」 등이 있다. 전자서명 및 인증 관련 법령으로는 「전자정부법」, 「전자서명법」 등이 있고, 정보통신망과 정보시스템의 보호조치 관련 법령으로는 「국가정보화기본법」, 「정보통신기반보호법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「전자거래기본법」, 「전자무역 촉진에 관한 법률」, 「산업기술혁신촉진법」, 「물류정책기본법」 등이 있다. 침해행위의 처벌에 관한 법령으로는 「정보통신기반보호법, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「전자무역촉진에 관한 법률」, 「물류정책기본법」 등이 있고, 개인정보보호 관련 법령으로는 「개인정보보호법」, 「전자정부법」, 「주민등록법」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」, 「신용정보의 이용 및 보호에 관한 법률」, 「금융실명거래 및 비밀보장에 관한 법률」 등이 있다.

3.2 '안전국가' 관련 법령의 한계

3.2.1 '안전국가' 법구조의 비체계성

우리나라의 국가의 안전과 관련된 입법은 그 체계성이 매우 낮다. '기본법'이라는 법명을 가진 관련 법령이 개별 재난영역을 규율하는 규범으로 존재하기도 하며, 재난영역별로 많은 법률이 제정되어 있고, 위험 또는 안전관리, 재난관리를 직접 규율하는 개별조항들도 '특별법', '기본법', '대책법' 등 다양한 형태로 각각의 법률에 산재되어 있다. 이러한 다양한 형태의 안전국가 법구조의 비체계성을 극복해야할 필요가 있다.

현재 제정되어 있는 위기관리의 기본법이라 할 수 있는 「재난 및 안전관리기본법」은 국가의 위기관리에 전체적으로 적용되는 기본원칙이나 표준화를 위한 개념, 용어의 통일 등 기본법이 수행해야 하는 일련의 기능을 담당하지 못하고 있으며, 위기관리분야의 기본법의 역할을 매우 제한적으로 수행하고 있거나 기본법이 담당해야 할 내용 이외에 지나치게 구체적인 내용의 규율을 함으로 인하여 다른 재난분야의 입법이 이 기본법을 준거로 스스로를 개선할 기회를 차단하고 있다. 예컨대, 「재난 및 안전관리기본법」은 '재난'이라는 용어를 사용하고 있으나, 「자연재해대책법」은 재난이라는 용어를 사용하지 아니하고 '재해'라는 용어를 사용하고 있다. 하지만 양자는 동일한 의미를 가진다. 또한 재난의 의미도 분야별 법률마다 달리 이용되고 있으며 여러 법률이 규율하고 있는 재해 혹은 재난의 유형도 개별 법률마다 달리 적용범위를 정하고 있다. 특히, 위기관리기본법의 부재 혹은 재난관리기본법의 기본법으로서의 기능 상실은 매우 복잡하게 제정되고, 도입된 각종 관련법제도를 연결하고, 예방중심의 안전관리와 대응중심의 재난관리를 연결하는 연결고리를 모호하게 하는 결과를 초래한다.

「재난 및 안전관리기본법」에서 천명하고 있는 주된 내용은 '대응' 체제이다. 물론 '안전관리'에 대한 개념도 있고, 예방관리를 위한 원칙도 규율되어 있기는 하다. 그러나 현재의 법률을 검토해 보면 위험원에 대한 안전관리는 개별 법률과 개별부처의 특정 규정으로 두면서, 기본법에서는 안전관리위원회에 대한 규정과 안전관리계획을 통하여 안전관리 업무를 '가정(假定)의 상태'에서 수행할 뿐이다. 이에 비해 대응에 대한 법규정은 비교적 상세하게 규

정되어 있으며, 직접 긴급구조의 행위자를 지정하는 등 비교적 상세하고 체계적으로 규율되어 있다.

이러한 현실은 개별법에 산재해 있는 재난위험요인 별 안전관리 기능과 재난의 대응 기능 간 연계고리를 설정해 두지 않아 특정한 분야에서 발생한 사고나 재난이 대형화하는 과정에서 예방과 대응간 연계관리를 어렵게 만들고 있다. 예컨대, 아현동 가스폭발현장에서 가스안전을 관리하는 가스공사 및 산업자원부와 재난응급대응을 담당하는 소방방재청, 구조대간 정보교환과 연계가 잘 이루어지지 않아 2차폭발의 위험을 제대로 관리하지 못하는 문제를 야기하거나, 숭례문 방화사건에서도 문화재의 안전관리를 담당하는 문화재청과 화재에 대응하는 소방서간 연계가 이루어지지 않아 적절한 대응이 어렵게 되는 결과를 초래하는 것이다. 또한 이러한 대응중심의 법체계는 위험성 및 취약성의 관리를 통한 재난관리의 효율성 제고의 기회를 사전적으로 위기관리당국이 포기하는 결과를 초래하고 있으며, 재난중심의 위기관리의 1차적인 책임자로서 지방자치단체의 역량을 약화시키는 가장 중요한 요인으로 작용하고 있다. 특히, 대응중심의 법률체계는 실제 대응현장에서 일차적인 위기관리 책무가 있는 지방정부와 재난대응책임기관의 역할모호성과 결부되어 위기관리 입법의 치명적인 한계를 노정한다.

3.2.2 물리적 안전과 사이버 안전 법제의 연계 미흡

안전국가를 구현하기 위한 활동으로는 외적 공격으로부터 국토를 지키는 국방, 전기・수도・가스・철도・도로 등 국민생활기반의 시설보호, 폭풍・호우・대설・홍수・해일・지진 등과 같은 자연재해 및 화재・폭발・방사성물질의 방출 등과 같은 인위적 사고에 대한 방재활동이 포함된다. 전쟁에 대한 대응이나 천연재해 및 사고에 대한 방재활동은 각각 국가안보와 질서유지의 가장 전형적인 활동이다. 하지만 국민생활기반시설에 대한 사이버공격으로 국민생활기반을 파괴시키거나, 방송・통신・금융 등 국가주요산업의 전산망을 교란・마비시키거나, 첨단무기체계를 교란시켜 이들을 무기력하게 만드는 등의 사이버침해는 종래의 '국가안전보장' 및 '질서유지'라는 2원적 분류방식으로는 적절한 대응이 불가능하다. 앞서 언급한 바와 같이 이러한 사이버 침해는 직・간접적으로 물리적 안전과 관련되며 방재, 재난으로 연계될 수 있다.

그러나 국내 '안전국가' 관련 법령은 물리적 안전 및 사이버 안전과 관련된 법령이 유기적으로 연계되지 않고 각각 별개로 규정되어 있다. 양자가 연계점 없이 각각 개별 법률의 목적에만 의존하고 있어 사이버 침해가 물리적 재난과 복합적으로 표출되는 위기현상에 대한 즉각적 대응이 미흡할 수밖에 없다.

따라서 이에 대한 입법 방향이나 추진체계의 개편은 불가피하다. 하지만 여전히 종래의 분류방식에 따라 종래 오프라인에서 정책을 수행하던 부처나 기관이 사이버공격에 대해서도 각각 대응하다 보니 사각지대의 발생은 물론, 날로 심각해져가는 사이버공격을 제대로 방어하지 못하고 있는 실정이다. 개별 소관부처의 극대화된 역량을 통합하여 국가차원의 사이버전 대응능력의 극대화가 이루어지지 못할 뿐 아니라 사이버전에 대비하는 국가정책 또한 임시처방형식으로서 일관성을 상실하고 있다[23]. 따라서 대한민국의 가장 중요한 국가정책이라 할 수 있는 '안전국가'를 실현하기 위해서는 사이버안전과 물리적 안전을 연계할 수 있는 입법상의 조치가 필요하여 사이버안전의 정책방향과 추진체계를 새롭게 개편할 필요가 있다.

4. '안전국가'의 규범체계 정립방향

4.1 안전국가 법제의 핵심원리로서 '사이버 안전 기본 규범원칙' 확립

안전국가의 측면에서 본다면 사이버 안전이라 함은 위기시 뿐만 아니라 평상시의 질서유지도 포함된다. 앞서 살펴보았듯이 현재 사이버 안전에 관한 개별 법률들이 산재되어 체계화되어 있지 못

하며 법률 간의 협력 및 연계도 제대로 이루어지지 못한 실정이다. 따라서 전통적 안보 차원, 국가 핵심기반 차원, 국민생활 안전 차원 등에서의 국가 사이버 위기를 포괄할 수 있는 기준이 되는 법률의 제정을 통하여 국가 사이버 위기관리와 관련된 법률을 체계화하는 것이 요구된다[1]. 이와 관련하여 사이버 안전 법규에 공통원칙으로 반영될 수 있는 기본규범의 확립이 우선적으로 선행될 필요가 있다. 미국은 오바마 대통령 출범과 함께 사이버공간 보안을 위한 5가지 전략분야를 수립, 시행하고 있으며[29], 이는 우리가 사이버 안전을 위한 기본규범 수립 시 참조 할만하다. 5가지 전략 프레임워크에는 「1) 백악관, 연방 차원의 최상위 리더십에 기반 한 강력한 추진 2) 지속적 혁신과 경기회복을 위한 디지털 국가 역량 축적 3)민간과 협력, 국제사회와의 공조를 통한 사이버 안보에 대한 책임 분배 4)사이버 위협에 대한 효과적 대응을 위한 정보공유·프레임워크 구축 5)혁신적 보안정책」 등이 포함된다.

국제적으로도 인터넷을 이용한 모든 범죄행위(컴퓨터 시스템·데이터 불법 접속, 지적재산권 침해, 바이러스 개발·유포, 아동 포르노그래피 배포, 컴퓨터 네트워크를 통한 사기·돈세탁·테러리즘 모의 등)를 규정한 '사이버범죄 조약(부다페스트 조약)' 등 사이버 안전에 있어서의 공동규약 마련하고 있다.

우리도 우리나라 고유의 실정을 반영할 수 있는 '사이버 안전 규범원칙'을 확립하고 이를 '안전국가' 관련 법령에 반영할 필요가 있다. 그 주요 내용으로는 선진국, 국제규범 등에 비추어 「1)글로벌 상호운용성, 2)네트워크 안정성, 3)신뢰 기반의 접속, 4)다자간 협력 거버넌스, 5)국가의 의무로서 사이버안전」 등이 고려될 수 있다.

4.2 안전국가 확립을 위한 통일적 추진체계 마련

안전국가 확립을 위해서는 사고·재난발생시 일사천리로 일관된 대응을 할 수 있도록 정부·민간 및 국가 간 협력기반 법제화가 필수적으로 요구된다. 현재 각 부처와 기관들은 사고의 성격(주요 취약점, 범죄형 공격, 군사 사고)에 따라 주도적인 대응 역할을 전담 또는 분담하나, 이를 제대로 구분하기도 힘들고 누가 주도해야 하는지 불분명하다. 즉 우리나라는 안전국가 기능이 여러 기관에 분산되어 있으며, 업무를 조정·총괄하는 컨트롤 타워가 불분명하다[20]. 특히 사이버위기 대응기관으로는 국가정보원의 국가사이버안전센터, 국방부의 사이버사령부, 한국인터넷진흥원의 인터넷침해대응센터를 주축으로 대검찰청 인터넷범죄수사센터, 경찰청 사이버테러대응센터, 국가보안기술연구소, 정보공유분석센터(ISAC) 등 다양하나 협력체계가 긴밀하지 못하며 각 주체들이 저마다 전문 지식과 법적 권한을 가지고 있으므로 이들을 하나의 조정 체계로 통합하기 위해서는 법적 뒷받침이 필요하다[1]. 최근 「국가 사이버안보 마스터 플랜('11.8.8)」을 통해 '국가사이버안전센터'를 중심으로 국가정보원의 컨트롤타워 기능과 부처별 역할을 명확히 하였으나, 이는 '행정계획' 수준으로 구체적 집행력 의문이다. 또한 「국가위기관리지침(대통령훈령 제229호)」에 따라 소방· 방재·사이버·교통 등 30여 개의 분야에 대한 위기관리가이드라인이 작성·배포되었으나 이러한 가이드라인은 해당 기관에 대한 법적 구속력이 없을 뿐만 아니라 가이드라인의 준수를 지휘·감독할 추진주체도 법정화되어 있지 못한 실정이다. 따라서 "권한을 행사하는 기관"이 아니라 "책임을 지는 기관"으로서 컨트롤타워 및 추진체계의 법정화가 필요하다. 특히 국가 사이버안전을 책임지는 조직은 다음 기능을 수행하는 것이 필요하다. 첫째, 국가 사이버 안전에 관한 중요 정책의 심의 및 총괄·조정, 둘째, 국가 사이버 안전 체계 및 경보·연습·평가 등 제도의 구축에 관한 기획 및 조정, 셋째, 국가 사이버 안전 기관이 수행하는 위기관리 업무의 협의와 조정, 넷째, 국가 사이버 위기 발생 시 통합 대응 기능의 수행 및 조정, 다섯째, 국가

사이버 위기 발생 이전에 이를 예방하기 위한 정책의 수립・집행 및 조치 사항, 여섯째, 국가 사이버 위기의 발생에 따른 각 기관별 소관 업무와 관련되는 응급대책의 수립・시행, 일곱째, 국가 사이버 위기 발생으로 인한 피해 복구 및 안정화 대책 등이 그것이다[1].

이와 관련하여 미국에서도 사이버 사고에 대한 연방의 책임은 여러 부처와 기관에 분산되어 있는데, 이는 현행 법률이 국가 안보와 기타 연방 네트워크의 보안을 구분하고 있기 때문이라는 지적은 참고 할만하다[29].

따라서 국민생활기반 파괴, 방송・통신・금융 등 국가주요기간산업 전산망 마비, 첨단무기체계 교란 등의 사이버침해에 대하여는 종래 '국가안전보장' 및 '질서유지'라는 2원적 분류방식으로는 대응이 불가능하며 사이버안전 추진체계는 소방방재청, 한국시설관리공단 및 각급 지방 시설물관리공단 등 재난・방재시스템과의 연계 되어야 하고 이를 위해 기관 간 위기관리 대응에 적극 협력하고 정보를 교환할 수 있도록 관계 법령 정비가 필요하다.

4.3 순기능을 증진시키기 위한 법제도 마련

한편 안전국가의 종합적 규범 확립의 일방향으로서 안전국가에 정보기술이 미치는 긍정적 효과를 배가할 수 있도록 각종 사회안전장치 및 재난・재해에 IT를 적극 활용할 수 있는 법제도적 기반 마련이 필요하다.

교량・터널・가스관・전기선로에 계측센서 부착 등 시설물의 실시간 계측 및 계측을 위한 시설 운영에 관한 구체적 규정 마련하는 것도 개선방안이 될 수 있다. 무선을 이용한 자동화재감시 시스템 적용에 대한 법적 근거, 하천수질 실시간 측정방법에 대한 구체적인 규정 마련 등 국가 기반시설에 대한 모니터링을 위한 시설물 설치에 대한 근거를 마련하고 그 운영에 대한 구체적 규정을 마련하는 것이 필요하다. 또한 이러한 기반시설에 대한 정보기술의 적용이 확장되기 위해서는 안전, 재해 관련 정보기술 적용 기업에 대한 행정처분 경감 및 국고지원 등의 인센티브 부여방안도 고려해 볼 만 하다. 특히 구조대원들에 대한 휴대용 기기(PAD)지원, 구조본부(Back-end)를 통한 통합된 재난정보 구조원들 간에 교환 등 재난재해 발생시 모바일・소셜서비스를 활용할 수 있는 적극적 법적 지원방안 마련도 필요하다.

4.4 역기능을 보완할 수 있는 법제도 개선

정보기술의 확산이 안전국가에 미치는 역기능을 예방하고 재난에 대한 대응, 복구가 원활히 이루어 질 수 있도록 법적 개선이 필요하다.

안전국가 관련 법령은 재난・재해 등에 대한 물리적 방재법령과 사이버침해에 대한 사이버안전법령이 상호 유기적으로 연계되지 않고 각각 별개로 규정・운영되고 있음을 지적하였다. 따라서 사이버 침해가 물리적 재난과 복합적으로 표출되는 위기현상에 즉각 대응하기 위한 체계가 미흡하므로 '물리적 안전법제'와 '사이버 안전 법제'의 연계, 융합, 체계화가 반드시 필요하다. 예컨대 사이버침해로 인한 제 2차적 침해로서 재난・재해 등과 같은 물리적 위험이 발생할 수 있는 바, 사이버위기관리체제, 즉 침해의 예방, 탐지, 대응 등에 물리적 재난・재해에 대한 관리체계를 포함하도록 법제를 개선하여야 할 것이다.

다음으로 위기에 대한 사전예방과 재난에 대한 대응 및 복구가 일목요연하게 집행될 수 있는 법체계 확립이 필요하다. 앞서 언급한 바와 같이 현행 국가안전 규범체계는 예방체계와 대응, 사후복구 체계가 끊김 없이 연계되어 있는 것이 아니라, 각각 개별적으로 규정되어 있어 재난에 대응하는 법 수범자와 법집행자 모두에게 혼란을 야기하고 있다. 즉 개별법에 산재해 있는 재난위험요인 별 안전관리 기능과 재난의 대응기능 간 연계고리를 설정해 두지 않아 사고나 재난이 대형화 되는 과정에서 예방과 대응 간 연계관리가 곤란하다.

따라서 '안전국가' 법체계, 표준화, 기본 용어 개념에 대한 체계화가 필요하다. 현재 위기관리기본법이

라 할 수 있는 「재난 및 안전관리기본법」은 국가위기관리에 전체적으로 적용되는 기본원칙이나 표준화를 위한 개념, 용어의 통일 등 기본법이 수행해야 하는 일련의 기능 부여하되, 단지 위기관리조직과 대응에 대한 부분적인 규정 및 국가기반위기에 대한 규율로 그 적용영역을 한정하고, 개별법에 산재해 있는 재난위험요인 별 안전관리 기능과 재난의 대응 기능 간 연계고리를 설정하는 것이 필요하다.

5. 결 언

위기와 기회는 함께 존재한다. 정보기술의 발달은 우리에게 좀 더 편리하고 윤택한 삶을 제공하며, 다양한 기회를 제공하기도 하지만 그 이면에는 위기도 함께 있다. 기회는 살리고 위기는 극복해야 한다. 그리고 이러한 위기를 극복하기 위한 국가기능의 핵심은 관련 법규범이다. 국가 안전을 위한 공행정작용은 당연히 법규범에 근거하여 이루어지게 된다. 그러나 현행의 법규범은 사이버공간의 안전이 물리적 위험과 연계된다는 정보기술의 변화환경을 적절히 반영하지 못하고 있으며 위기에 대한 대응법령체계 역시 혼란스럽다. 따라서 본 고에서는 이러한 문제의식을 기반으로 국가의 안전에 대한 통일적·체계적 법규범 정립을 위한 시론적 연구로서 '안전국가'에 대한 새로운 법적 개념정립을 제안하였다. 사이버공간의 특성상 외부적 공격과 내부적 위험에 각각 따로 대응한다는 것은 거의 불가능한 일이다. 그러나 외부적 '국가안전'은 외적 위협이나 침략으로부터 국가의 안전을 지키는 것으로 통용되고 있는 현실을 인정한다면 이러한 외적 안전은 물론이고 국민생활기반시설을 보호하고 천재지변 등의 재해를 예방·극복하는 등의 내부적 안전까지도 모두 포함하여 국민들이 안락·평온한 상태에서 헌법상 기본권을 향유할 수 있도록 하는 국가 공행정작용을 포괄할 수 있는 새로운 개념의 형성이 필요하다. 본 고에서는 이러한 개념을 이른바 "안전국가"로 정의하고 이러한 안전국가의 규범체계의 한 개와 개선방향을 도출하고자 하였다. 우리나라의 현행 안전국가 법규체계는 대응중심의 법률체계, 재난위험요인 별 안전관리 기능과 재난의 대응 기능 간 연계고리 미흡 등으로 인해 특정한 분야에서 발생한 사고나 재난이 대형화하는 과정에서 예방과 대응 간 연계관리를 어렵게 만들고 있다. 또한 사이버안전과 물리적 안전을 연계할 수 있는 입법상의 조치가 미흡하여 사이버공격에 대한 사각지대의 발생은 물론, 날로 심각해져가는 사이버공격을 제대로 방어하지 못하고 있는 실정이다. 이러한 한계를 극복하기 위하여 안전국가 법제의 핵심원리로서 '사이버 안전 기본 규범원칙' 확립 및 안전국가 확립을 위한 통일적 추진체계 마련을 제안하였다. 또한 정보기술의 확산이 안전국가에 미치는 역기능을 예방하고 재난에 대한 대응, 복구가 원활히 이루어 질 수 있도록 법제도 개선방향을 제안하였다. 그리고 정보기술이 주는 '기회'를 살릴 수 있도록, 즉 안전국가에 정보기술이 미치는 긍정적 효과를 배가할 수 있도록 각종 사회안전장치 및 재난·재해에 정보기술을 적극 촉진하도록 하는 법제도 개선을 제안하였다.

참 고 문 헌

[1] 강석구 외 6인, 「사이버안전체계 구축에 관한 연구」, 한국형사정책연구원, 2010, pp.282-307.

[2] 권문택, "국가사이버안전관리 조직의 통합적 체계구축에 관한 연구", 「정보·보안논문지」 제9권, 제3호(2009), pp.61-70.

[3] 권영성, 「헌법학원론」, 법문사, 2007.

[4] 김귀남, "국가 사이버전 대비방안 연구", 「정보·보안논문지」, 제6권, 제4호(2006), pp.141-151.

[5] 김민식 외, "통합적 사이버 위기관리 체계의 필요성에 관한 연구 : 미국과 한국의 제도 및 정책 비교를 중심으로", 「정보·보안논문지」, 제9권, 제1호(2009), pp.29-37.

[6] 김민호, "지식정보사회에서 행정법학의 새로

운 패러다임 모색", 「공법학연구」 제8집, 제3호(2007), pp.97-100.
[7] 김민호, "차세대 전자정부의 공법적 과제", 「토지공법연구」, 제48집(2010), pp.184-185
[8] 김민호, "전자기파 공격 철저히 대비해야", 서울신문, 2012. 6. 18.
[9] 김민호, "사이버보안 관련법령 정비 서둘러야", 서울신문, 2011. 12. 26.
[10] 김인중, "사이버범죄 추적·수사기법과 문제점 분석", '사이버안전 확보를 위한 바람직한 연구방향'(전문가초청 워크숍 자료집), 한국형사정책연구원, 2010, p.42.
[11] 김인중, 이철원, 임을규, "사이버테러리즘의 변화 : 자생적테러와 대응방안", ICCSA 2007, LNCS(SCI-E), 2007.
[12] 김준호(역)/Ulrich Sieber(저), "전세계 사이버 공간상의 복합성에 대한 대처방안 : 컴퓨터관련형법의 조화", 「Law and technology」, 서울대학교 기술과법센터, 제5권, 제4호(2009), pp.3-44.
[13] 김홍석, "사이버 테러와 국가안보", 「저스티스」 통권 제121호(2010년), pp.319-356.
[14] 두산백과사전; available at http://100.naver.com/100.nhn?docid=830869.
[15] 박동균, "북한의 사이버 테러공격 가능성 및 대비전략", 「국가위기관리학회보」, 제1권(2009), pp.53-66.
[16] 손경한·박진아, "사이버 불법행위에 대한 국제적 규제", 「법학논문집」, 제31집, 제1호(2007), pp.549-581.
[17] 안철현, "국가 위기관리 개념의 변화와 위기관리 체계의 구축방향", 「비상기획보」, 제73호(2005), pp.14-28.
[18] 우희철, "미래 정보전에 대비한 육군전술지휘정보체계(C4I) 정보보호대책 연구", 「디지털정책연구」, 제10권, 제9호(2012) pp.1-13.
[19] 이상호, "사이버전의 실체와 미래 사이버공격 대응방안 : 7.7사이버공격의 교훈과 대책", 「시대정신」 제44호(2009), pp.246-265.
[20] 이재은 외 2인, "국가 사이버위기 관리 체계 강화방안에 관한 연구", 「한국위기관리논집」, 제4권, 제2호(2008) pp.69-93.
[21] 이창범, "유럽연합의 정보보안 및 개인정보보호 법제 현황", 「인터넷법률」, 법무부, 제38호(2007), pp.75-108.
[22] 이철수, "침해사고 국가 대응 체계-National security system for countering information incidents", 「정보보호학회지」, 제15권, 제1호(2005), pp.36-38.
[23] 정준현, "국가 사이버안보를 위한 법제 현황과 개선방향", 「국가정보연구」, 제4권, 제2호(2011), pp.99-100.
[24] Brenner, Susan W., "Cybercrime and the U.S. Criminal Justice System, Global Perpectives in Information Security : legal, social, and international issues", John Wiley and Sons, 2009.
[25] Congressional Research Service, Department of Homeland Security Reorganization : The 2SR Initiative, 2005.
[26] Harley, B., A Global Convention on Cybercrime?, 2010.
[27] Lewis, James A., The "Korean" Cyber Attacks and Their Implications for Cyber Conflict, Center for Strategic and International Studies, 2009.
[28] Stern. K., Das Staatsrecht der Bundesrepublik Deutschland, Bd. II, 1980, S. 1468ff.
[29] White House, "Cyberspace Policy Review : Assuring a Trusted and Resilient Information and Communications Infrastructure", 2009. pp.7-35.
[30] White House, National Strategy for Trusted Identities in Cyberspace(NSTIC)-Creating Options for Enhanced Online Security and Privacy(Draft), 2010. 6.

◈ 저 자 소 개 ◈

김 현 경(ksbs1801@nia.or.kr)

현재 한국정보화진흥원(NIA) 책임연구원으로 재직 중이며, 관심분야는 정보기술과 관련된 법제, 지식재산 관련 법제, 정보보호 법제 등이다.